INVESTIGATION REPORT

I Sent NameSilo 20+ Abuse Reports About a Crypto Scammer. Here's What Happened.

A documented account of 20+ delivery-receipted abuse reports submitted to NameSilo about xmrwallet.com between 2023-2026 — and NameSilo's public response calling the operator 'the victim of a hack' while three other registrars suspended identical domains within days.

#security · #webdev · #domainnames · #cryptocurrency

Canonical source:
https://phishdestroy.eth.limo

Arweave permanent backup (tamper-evident):
https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

Evidence archive (SHA-256 verified screenshots):
github.com/phishdestroy/namesilo-xmrwallet-coverup

All evidence in this document is released for unrestricted use in legal, regulatory, and law enforcement proceedings. No authorization required. Cite freely.

PUBLISHED BY
PhishDestroy Research
report@phishdestroy.io

PERMANENT ARCHIVE
phishdestroy.eth.limo
github.com/phishdestroy

EVIDENCE LICENSE
Open — cite freely
Legal / regulatory / LE use OK

> *I want to tell you about something that happened when I tried to report a crypto scammer to his domain registrar — NameSilo (CSE:URL). Not what I expected to happen. What actually happened.*

Evidence archive: https://github.com/phishdestroy/namesilo-xmrwallet-coverup

Full investigation: https://phishdestroy.eth.limo

Permanent record: https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

---

The Background

xmrwallet.com is a Monero web wallet that has been operating since approximately 2016. In 2023, network-level analysis revealed the site was transmitting users' private view keys to its servers and substituting sweep transactions for the ones users signed. The technical evidence is specific:

- `session_key = [blob]:[base64(address)]:[base64(viewkey)]` — your private view key, in every session token
- `raw_tx_and_hash.raw = 0` — your signed transaction, discarded
- `type == 'swept'` — the server's own sweep of your funds

This is not a misconfiguration. It is not a vulnerability. It is the product. The theft code is the website.

The site has confirmed victims. 590 XMR stolen from one user. 17.44 XMR stolen from another, with TX ID and key documented and independently verified. At least 40 named victims in Reddit alone, 60% of whose posts were later deleted by DMCA threats from the operator.

The operator is identified. The infrastructure is documented. The evidence is public.

The Reports

Between 2023 and 2026, PhishDestroy submitted **20+ abuse reports** to NameSilo through their official abuse handling portal. Not emails to random addresses. Reports through the system NameSilo specifies in their abuse policy. With delivery receipts.

Each report included:

- The domain
- A description of the abuse
- Technical evidence
- Contact information

This is what you're supposed to do. Report abuse to the registrar. Follow the process. Document the reports.

The Response — or the Absence of One

For three years, across 20+ reports: nothing.

No acknowledgment of evidence. No action on the domain. No suspension. No response explaining why the reports were insufficient.

Meanwhile, the site kept running. More users lost funds.

What Other Registrars Did

In early 2026, the same evidence was sent to registrars holding other xmrwallet domains — xmrwallet.cc, xmrwallet.biz, xmrwallet.net.

Registrar	Domain	Result	Timeframe
PublicDomainRegistry	xmrwallet.cc	**Suspended**	Days
WebNic	xmrwallet.biz	**Suspended**	Days
NICENIC	xmrwallet.net	**DNS killed**	Days
NameSilo	**xmrwallet.com**	**Not suspended**	**Never**

Same evidence. Same operator. Three registrars acted in days. One did not act in three years.

The Statement

On March 13, 2026, NameSilo published a public statement on Twitter.

It called the operator of xmrwallet.com **"the victim of a hack."**

It stated that **"prior to that, we had received no abuse reports."**

It stated that their review was conducted **"not involving the registrant."**

It stated they were **"working with the registrant to remove the website from VT reports"** — helping the operator scrub his VirusTotal security warnings while the site was still live and actively stealing.

Each of these four claims is contradicted by documented evidence. The delivery receipts for 20+ prior reports were submitted to ICANN Contractual Compliance five days later.

Archived statement: https://ghostarchive.org/archive/CXXZ0

The Operator's Own Words

Before NameSilo published their statement, the operator had emailed PhishDestroy directly.

February 16, 2026:

> *"There is no phishing going on… we don't store seeds or keys, everything is done in your browser locally."*

He never claimed a hack. He claimed the site was legitimate.

February 17, 2026:

> *"Feel free to subpoena the domain registrar for my information."*

Someone says that line when they're confident their registrar is on their side. Three days before NameSilo called him "the victim."

February 23, 2026 (same day two of his other domains were suspended by other registrars):

> *"I've hired a lawyer and a private investigator."*

No lawyer appeared. No action was filed.

What Happened to Our Research Account

After publishing rebuttals to NameSilo's statement on Twitter/X, PhishDestroy's research account — a verified Gold account — was locked.

X Support emailed twice:

1. "violation against inauthentic behaviors — will not overturn" (no tweet cited, no rule cited)
2. Three weeks later — subject line: **"Your account has been restored"** — "Our automated systems have determined there was no violation"

The account is still locked. X's automation cleared it. A human agent — responding to what the evidence pattern suggests was a Gold Checkmark corporate complaint — overrode the automation.

No-violation email · **"Restored" email**

The Ending

xmrwallet.com has since been transferred from NameSilo to Namecheap. Not suspended. Transferred. The operator chose to leave; NameSilo facilitated the transfer rather than enforcing its abuse policy.

The site continues to operate. The theft mechanism, as far as can be determined from external signals, is unchanged.

The ICANN complaint is open. All evidence is public. Everything is on record.

If you're a developer, sysadmin, or security researcher evaluating NameSilo as a registrar: the above is documented fact. The delivery receipts exist. The statement is archived. The other registrars' actions are on record.

Sources

- **Full investigation:** https://phishdestroy.eth.limo
- **Evidence archive:** https://github.com/phishdestroy/namesilo-xmrwallet-coverup
- **NameSilo statement (archived):** https://ghostarchive.org/archive/CXXZ0
- **ICANN complaint portal:** https://www.icann.org/compliance/complaint
- **Technical breakdown:** https://phishdestroy.eth.limo/xmrwallet-research.html
- **Permanent archive:** https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

Contact: report@phishdestroy.io

All Sources & Permanent Mirrors

Primary investigation site: *https://phishdestroy.eth.limo*

Evidence archive (60+ SHA-256 verified screenshots):
https://github.com/phishdestroy/namesilo-xmrwallet-coverup

Technical GitHub repo (xmrwallet theft code analysis):
https://github.com/phishdestroy/DO-NOT-USE-xmrwallet-com

Arweave permanent backup — tamper-evident, no takedowns:
https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

IPFS mirror (4everland): *https://ipfs-archive-pbojso5s-phishdestroy.ipfs.4everland.app/*

NameSilo statement (GhostArchive — immutable): *https://ghostarchive.org/archive/CXXZ0*

ICANN Contractual Compliance complaint: *https://www.icann.org/compliance/complaint*

URLScan public records (63+ scans of xmrwallet.com):
https://urlscan.io/search/#domain:xmrwallet.com

VirusTotal: *https://www.virustotal.com/gui/domain/xmrwallet.com*

Contact: *report@phishdestroy.io*